CYBERCRIME
(KEJAHATAN BERBASIS KOMPUTER)

Alcianno G. Gani
localghost2000@yahoo.com

ABSTRACT

Information technology plays an important role, both in the present and in the future. The Internet is one part of the development of information technology that has opened new horizons in human life. The Internet can be interpreted as an information and communication space that penetrates the boundaries between countries and accelerates the spread of science and simplifies all human activities.

However, every positive side must have a negative side. The Internet applies in this case many crimes that can occur in cyberspace called cybercrime. Currently, we cannot feel the word "safe" in the cyber world. Various countermeasures that are considered effective are still being done to date, although not avoiding Cybercrime perpetrators, at least it can downplay the possibility of someone becoming one of the victims of Cybercrime or countermeasures when Cybercrime occurs.

With so many emerging Cybercrime, a law is urgently required. The right laws and methods to prevent Cybercrime.

***Keywords**: Internet, Cyberspace, Cybercrime, Cyber, Law.*

ABSTRAK

Teknologi informasi memegang peran yang penting, baik di masa kini maupun masa yang akan datang. Internet adalah salah satu bagian dari perkembangan teknologi informasi yang telah membuka cakrawala baru dalam kehidupan manusia. Internet dapat diartikan sebuah ruang informasi dan komunikasi yang menembus batas-batas antarnegara dan mempercepat penyebaran ilmu pengetahuan serta mempermudah segala kegiatan yang dilakukan manusia.

Walaupun begitu, setiap sisi positif pasti memiliki sisi negative. Internet berlaku dalam hal ini banyak kejahatan yang dapat terjadi dalam cyberspace yang dinamakan cybercrime. Saat ini, kata "aman" belum dapat kita rasakan dalam dunia cyber. Berbagai penanggulangan yang dianggap efektif masih dilakukan hingga saat ini, walaupun tidak menghindari para pelaku Cybercrime, setidaknya dapat mengecilkan kemungkinan seseorang menjadi salah satu korban dari Cybercrime atau penanggulangan saat Cybercrime terjadi.

Dengan begitu banyak Cybercrime yang muncul, diperlukan segera sebuah hukum. Hukum yang cocok dan metode preventif untuk mencegah Cybercrime.

***Keywords**: Internet, Cyberspace, Cybercrime, Cyber, Hukum.*

PENDAHULUAN

Internet sudah menjadi salah satu kewajiban dalam hidup saat ini. Kemudahan yang ditawarkan *Internet* semakin membuat manusia terlena. *Internet* menghubungkan setiap penggunanya. Tidak ada batasan waktu, wilayah ataupun *gender*. Teknologi Informasi saat ini seolah-olah menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kemajuan, kesejahteraan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Kebutuhan akan teknologi jaringan komputer semakin meningkat. Selain sebagai media penyedia informasi, melalui *internet* pula kegiatan komunitas komersial menjadi bagian terbesar dan pesat pertumbuhannya serta menembus berbagai batas Negara. Bahkan melalui jaringan ini, segala macam informasi di dunia bisa diketahui selama 24 jam. Melalui dunia *internet* atau bisa disebut juga *cyberspace*, apapun dapat dilakukan. Segi positif dari dunia maya ini tentu saja akan menambah trend dalam perkembangan teknologi dunia dengan segala bentuk kreatifitas manusia. Akan tetapi dampak negaif pun tidak bisa dihindari. Tatkala pornografi marak dimedia *internet*, masyarakat pun tak bisa berbuat banyak. Seiring dengan berkembangnya teknologi *internet*, menyebabkan munculnya kejahatan yang disebut dengan *cybercrime* atau kejahatan melalui jaringan *internet*.

Munculnya beberapa kasus *cybercrime*, seperti pencurian kartu kredit, *hacking* beberapa situs, menyadap transmisi data orang lain, misalnya *email* dan memanipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam program Komputer. Sehingga dalam kejahatan komputer dimungkinkan adanya delik formil dan delik materil. Delik formil adalah perbuatan seseorang yang memasuki Komputer orang lain tanpa ijin, sedangkan delik materil adalah perbuatan yang menimbulkan akibat kerugian bagi orang lain. Adanya *cybercrime* telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknoligo komputer, khususnya jaringan *internet*.

PENGERTIAN *CYBERCRIME*

Cybercrime atau kejahatan berbasis komputer, adalah kejahatan yang melibatkan komputer dan jaringan (*network*).[1] Komputer mungkin telah digunakan dalam pelaksanaan kejahatan, atau mungkin itu sasarannya.[2] *Cybercrimes* dapat didefinisikan sebagai: "Pelanggaran yang dilakukan terhadap perorangan atau sekelompok individu dengan motif kriminal untuk secara sengaja menyakiti reputasi korban atau menyebabkan kerugian fisik atau mental atau kerugian kepada korban baik secara langsung maupun tidak langsung, menggunakan jaringan telekomunikasi modern seperti *Internet* (jaringan termasuk namun tidak terbatas pada ruang *Chat*, *email*, *notice boards* dan kelompok) dan telepon genggam (*Bluetooth* / SMS / MMS)".[3] *Cybercrime* dapat mengancam seseorang, keamanan negara atau kesehatan finansial.[4] Isu

---

[1] *Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.*

[2] *Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.*

[3] *Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9*

[4] *Steve Morgan (January 17, 2016). "Cyber Crime Costs Projected To Reach $2 Trillion by 2019". Forbes. Retrieved September 22, 2016.*

seputar jenis kejahatan ini telah menjadi sangat populer, terutama seputar *hacking*, pelanggaran hak cipta, penyadapan yang tidak beralasan dan pornografi. Ada pula masalah privasi pada saat informasi rahasia dicegat atau diungkapkan, secara sah atau tidak. Debarati Halder dan K. Jaishankar lebih jauh mendefinisikan *cybercrime* dari perspektif *gender* dan mendefinisikan *"cybercrime against women"* sebagai "Kejahatan yang di-targetkan pada wanita dengan motif untuk secara sengaja menyakiti korban secara psikologis dan fisik, menggunakan jaringan telekomunikasi modern seperti *internet* dan telepon genggam". Secara sengaja, baik pemerintah dan swasta terlibat dalam *cybercrimes*, termasuk spionase, pencurian keuangan dan kejahatan lintas batas (*cross-border*) lainnya. Kegiatan yang melintasi batas negara dan melibatkan kepentingan setidaknya satu negara ter-kadang disebut sebagai *cyberwarfare*.

Sebuah laporan (disponsori oleh *McAfee*) memperkirakan bahwa kerusakan tahun-an yang disebabkan oleh *cybercrimes* pada ekonomi global mencapai $445 miliar.[5] Namun, sebuah laporan dari *Microsoft* menunjukkan bahwa perkiraan berbasis survei semacam itu "sangat tidak sempurna" dan membesar-besarkan keru-gian yang sebenarnya.[6] Sekitar $1,5 miliar hilang pada tahun 2012 untuk penipuan kartu kredit dan debit *online* di Amerika Serikat.[7] Pada tahun 2016, se-buah studi oleh Juniper Research mem-perkirakan bahwa biaya *cybercrime* bisa mencapai 2,1 triliun pada tahun 2019.[8]

KLASIFIKASI

Penipuan dan kejahatan finansial

Penipuan dengan menggunakan komputer adalah salah representasi fakta yang tidak jujur yang dimaksudkan untuk membiar-kan orang lain melakukan sesuatu yang menyebabkan kerugian. Dalam konteks ini, kecurangan tersebut dilakukan de-ngan cara:

- Mengubah dengan cara yang tidak sah. Ini memerlukan sedikit keahlian teknis dan merupakan bentuk pencurian umum oleh seorang karyawan yang mengubah data atau memasukkan data palsu atau dengan memasukkan in-struksi yang tidak sah atau meng-gunakan proses yang tidak sah.
- Mengubah, menghancurkan atau men-curi output, biasanya untuk menyem-bunyikan transaksi yang tidak sah. Ini sulit dideteksi;
- Mengubah atau menghapus data yang tersimpan.

Bentuk kecurangan lainnya dapat difasili-tasi dengan menggunakan sistem kom-puter, termasuk penipuan bank, *carding*, pencurian identitas, pemerasan dan pen-curian informasi rahasia.

Berbagai penipuan internet banyak ber-basis *phishing* dan *social engineering* yang menjadi sasaran biasanya konsumen dan pelaku bisnis.

Cyberterrorism

Pejabat pemerintah dan spesialis ke-amanan teknologi informasi telah men-dokumentasikan peningkatan yang signi-fikan dalam masalah Internet dan pemin-

[5] *"Cyber crime costs global economy $445 billion a year: report". Reuters. 2014-06-09. Retrieved 2014-06-17.*

[6] *"Sex, Lies and Cybercrime Surveys" (PDF). Microsoft. 2011-06-15. Retrieved 2015-03-11.*

[7] *"#Cybercrime— what are the costs to victims - North Denver News". North Denver News. Retrieved 16 May 2015.*

[8] *"Cybercrime will Cost Businesses Over $2 Trillion by 2019" (Press release). Juniper Research. Retrieved May 21, 2016.*

daian *server* sejak awal 2001. Namun, ada kekhawatiran yang berkembang di antara lembaga pemerintah seperti Biro Investigasi Federal (*Federal Bureau of Investigations* / FBI) dan Badan Intelijen Pusat (*Central Intelligence Agency* / CIA) bahwa intrusi semacam itu adalah bagian dari usaha terorganisir oleh *cyber-terrorist*, dinas intelijen asing atau kelompok lain untuk memetakan potensi celah keamanan dalam sistem kritis.[9] Seorang *cyberterrorist* adalah seseorang yang mengintimidasi atau menggalang pemerintah atau organisasi untuk memajukan tujuan politik atau sosialnya dengan meluncurkan serangan berbasis komputer terhadap komputer, jaringan atau informasi yang tersimpan di dalamnya.

Cyberterrorisme secara umum dapat didefinisikan sebagai tindakan terorisme yang dilakukan melalui penggunaan dunia maya atau sumber daya komputer (Parker 1983). Sebagai contoh, sebuah propaganda sederhana di Internet akan terjadi serangan bom saat liburan tahun baru bisa dianggap sebagai *cyber-terrorism*. Ada juga kegiatan *hacking* yang diarahkan pada individu atau keluarga yang diselenggarakan oleh kelompok-kelompok di dalam jaringan, cenderung menimbulkan ketakutan di kalangan orang-orang, mengumpulkan informasi yang relevan untuk menghancurkan kehidupan masyarakat, perampokan, pemerasan, dll.[10]

Cyberextortion

Cyberextortion terjadi saat sebuah situs *web*, *server e-mail* atau sistem komputer dikenai atau diancam dengan penolakan berulang (*Denial of Service* / DoS) terhadap layanan atau serangan lainnya oleh *hacker* jahat. Para h*acker* ini menuntut uang sebagai imbalan dengan janji akan menghentikan serangannya dan atau menawarkan "perlindungan". Menurut Biro Investigasi Federal, saat ini semakin banyak serangan yang dilakukan para pelaku *cyberextortion* pada situs *web* perusahaan dan jaringan, melumpuhkan kemampuan / kinerja mereka untuk beroperasi dan menuntut pembayaran untuk memulihkan layanan mereka. Lebih dari 20 kasus dilaporkan setiap bulan ke FBI dan banyak yang tidak dilaporkan untuk menjaga agar nama korban tidak keluar dan tersebar ke publik. Pelaku biasanya menggunakan serangan *denial-of-service* terdistribusi (*distributed denial-of-service* / DDoS).[11] Contoh *cyberextortion* adalah serangan terhadap perusahaan *Sony Pictures* pada tahun 2014.[12]

Cyberwarfare

Departemen Pertahanan Amerika Serikat (*Department of Defense* / DoD) mencatat bahwa dunia maya telah menjadi perhatian tingkat nasional melalui beberapa peristiwa terkini mengenai signifikansi *geo-strategis*. Di antaranya termasuk serangan terhadap infrastruktur Estonia di tahun 2007, yang diduga oleh *hacker* Rusia. "Pada bulan Agustus 2008, Rusia kembali melakukan serangan *cyber*, kali ini dalam kampanye kinetik dan non kinetik yang terkoordinasi dan disinkron-

[9] *Laqueur, Walter; C., Smith; Spector, Michael (2002). Cyberterrorism. Facts on File. pp. 52–53. Retrieved 5 December 2016.*

[10] *"Cybercriminals Need Shopping Money in 2017, Too! - SentinelOne". sentinelone.com. Retrieved 2017-03-24.*

[11] *Lepofsky, Ron. "Cyberextortion by Denial-of-Service Attack" (PDF). Archived from the original (PDF) on July 6, 2011.*

[12] *Mohanta, Abhijit (6 December 2014). "Latest Sony Pictures Breach : A Deadly Cyber Extortion". Retrieved 20 September 2015.*

kan melawan negara Georgia. Khawatir bahwa serangan semacam itu dapat menjadi norma perang antar negara di masa depan, dampak dari konsep operasi dunia maya akan disesuaikan oleh para komandan militer di masa depan.[13]

Komputer sebagai target

Kejahatan ini dilakukan oleh kelompok kriminal terpilih. Tidak seperti kejahatan yang menggunakan komputer sebagai alat, kejahatan ini memerlukan pengetahuan teknis sang pelaku. Dengan demikian seiring perkembangan teknologi, maka berkembang pula sifat kejahatannya. Kejahatan ini relatif baru dalam sejarah komputer, yang menjelaskan betapa tidak siapnya masyarakat dan dunia pada umumnya untuk memberantas kejahatan ini. Ada banyak kejahatan dari sifat ini yang dilakukan setiap hari di internet. Kejahatan yang terutama menargetkan jaringan komputer atau perangkat meliputi:

- *Virus* komputer.
- *Denial-of-service attacks*.
- *Malware* (*malicious code*)
- Dll.

Komputer sebagai alat

Bila individu merupakan target utama *cybercrime*, komputer bisa dianggap sebagai alat ketimbang target. Kejahatan ini umumnya kurang melibatkan keahlian teknis. Kelemahan manusia umumnya dieksploitasi. Kerusakan yang ditangani sebagian besar bersifat psikologis dan tidak berwujud, membuat tindakan hukum terhadap varian ini lebih sulit. Inilah kejahatan yang telah ada selama berabad-abad di dunia *offline*. Penipuan, pencurian, dan sejenisnya sudah ada bahkan sebelum pengembangan peralatan berteknologi tinggi. Penjahat yang sama hanya diberi alat yang meningkatkan potensi korbannya dan membuatnya semakin sulit dilacak dan ditangkap.

Kejahatan yang menggunakan jaringan komputer lainnya meliputi:

- Penipuan dan pencurian identitas (walaupun hal ini semakin banyak menggunakan *malware hacking* atau *phishing*, menjadikannya sebagai contoh kejahatan komputer "sebagai sasaran" dan "komputer sebagai alat").
- Perang informasi.
- Penipuan *phishing*.
- *Spam*.
- Pornografi, termasuk pelecehan dan ancaman.

Pengiriman *email* massal yang tidak diminta untuk tujuan komersial (*spam*) tidak sah di beberapa wilayah hukum. *Phishing* sebagian besar disebarkan melalui *email*. *Email phishing* mungkin berisi tautan ke situs web lain yang terpengaruh oleh malware. Atau, mungkin berisi tautan ke perbankan *online* palsu atau situs web lain yang digunakan untuk mencuri informasi akun pribadi.

Konten tidak senonoh atau menyinggung

Isi situs *web* dan komunikasi elektronik lainnya mungkin tidak menyenangkan, tidak senonoh atau menyinggung karena berbagai alasan. Dalam beberapa kasus, komunikasi ini mungkin legal. Sejauh mana komunikasi ini melanggar hukum sangat bervariasi di antara negara-negara lain. Ini adalah area sensitif di mana pengadilan dapat terlibat dalam arbitrase antar kelompok dengan keyakinan yang kuat. Salah satu bidang pornografi *internet* yang telah menjadi sasaran upaya

[13] *Dennis Murphy (February 2010). "War is War? The utility of cyberspace operations in the contemporary operational environment" (PDF). Center for Strategic Leadership. Archived from the original (PDF) on 20 March 2012.*

terkuat pada pembatasannya adalah pornografi anak yang ilegal dikebanyakan wilayah hukum di dunia.

Pelecehan

Dalam konten ini mungkin menyinggung dengan cara yang tidak spesifik, pelecehan mengarahkan kata-kata kotor, penghinaan atau komentar pada individu tertentu yang memusatkan perhatian pada jenis kelamin, ras, agama, kebangsaan atau orientasi seksual, atau biasa di sebut mengandung unsur SARA. Hal ini sering terjadi di *chat room*, melalui *newsgroup* dan dengan mengirim *email* kebencian ke pihak yang berkepentingan. Pelecehan di internet juga termasuk balas dendam .

Ada kasus di mana seseorang melakukan kejahatan menggunakan komputer dapat menyebabkan hukuman yang berat. Misalnya, dalam kasus di Amerika Serikat. Neil Scott Kramer, Kramer menjalani hukuman yang berat menurut Buku Pedoman Hukum Amerika Serikat 2.21(b)(3) yang menggunakan ponselnya untuk "membujuk, menarik atau memaksa anak di bawah umur untuk melakukan tindakan seksual terlarang." Kramer berpendapat bahwa klaim ini tidak mencukupi karena tuduhannya adalah membujuk melalui perangkat komputer dan telepon genggamnya secara teknis bukanlah komputer. Meskipun Kramer mencoba mengemukakan pendapat ini, Buku Pedoman Hukum AS menyatakan bahwa istilah komputer berarti “perangkat pengolah data kecepatan tinggi elektronik, magnetik, optik, elektrokimia atau kecepatan tinggi lainnya yang melakukan fungsi logika, aritmatika, atau penyimpanan dan mencakup fasilitas penyimpanan data apa pun atau fasilitas komunikasi yang berhubungan langsung dengan atau beroperasi bersamaan dengan alat tersebut."[14]

Connecticut adalah negara bagian AS yang mengeluarkan sebuah undang-undang yang juga mengkategorikannya menjadi tindak pidana untuk melecehkan seseorang melalui komputer. Michigan, Arizona, Virginia dan South Carolina juga telah mengeluarkan undang-undang yang melarang pelecehan dengan cara elektronik. [15][16]

Pelecehan sebagaimana didefinisikan dalam undang-undang komputer AS biasanya berbeda dari penindasan maya, karena yang pertama biasanya berhubungan dengan "penggunaan komputer atau jaringan komputer seseorang untuk berkomunikasi dengan bahasa vulgar, cabul, bernafsu, atau tidak senonoh, atau memberikan saran atau usulan sifat tidak senonoh atau mengancam tindakan ilegal atau tidak bermoral, "sementara yang terakhir tidak memerlukan sesuatu yang bersifat seksual.

Meskipun kebebasan berbicara dilindungi oleh undang-undang di kebanyakan masyarakat demokratis, namun tidak mencakup semua jenis pidato. Sebenarnya ucapan / teks ucapan "ancaman benar" dikriminalisasi karena "niat untuk menyakiti atau mengintimidasi", yang juga berlaku untuk ancaman jaringan atau topik terkait secara *online* dalam teks tertulis

[14] *"United States of America v. Neil Scott Kramer". Retrieved 2013-10-23.*
[15] *"1. In Connecticut, harassment by computer is now a crime". Nerac Inc. February 3, 2003. Archived from the original on April 10, 2008.*
[16] *"Section 18.2-152.7:1". Code of Virginia. Legislative Information System of Virginia. Retrieved 2008-11-27.*

atau ucapan.[17] Definisi Mahkamah Agung Amerika Serikat tentang "ancaman sebenarnya" adalah "pernyataan di mana pembicara bermaksud mengkomunikasikan ungkapan serius dari suatu niat untuk melakukan tindakan kekerasan yang melanggar hukum kepada individu atau kelompok tertentu".[20]

Perdagangan narkoba

Pasar gelap digunakan untuk membeli dan menjual obat-obatan terlarang secara *online*. Beberapa pedagang narkoba menggunakan alat pesan terenkripsi untuk berkomunikasi dengan pemasok narkoba. Situs *web* gelap *Silk Road* adalah pasar *online* utama untuk obat-obatan sebelum dimatikan oleh penegak hukum (kemudian dibuka kembali di bawah manajemen baru, dan kemudian ditutup oleh penegak hukum lagi). Setelah *Silk Road 2.0* turun, *Silk Road 3 Reloaded* muncul. Namun sebenarnya itu hanya pasar yang lebih lama yang bernama *Diabolus Market*, yang menggunakan nama tersebut untuk lebih banyak menarik keuntungan dari kesuksesan merek sebelumnya.[18]

CYBERATTACKS

Cyberattacks atau Serangan *cyber* adalah jenis manuver ofensif yang digunakan oleh negara-negara, individu, kelompok, atau organisasi yang menargetkan sistem informasi komputer, infrastruktur, jaringan komputer dan atau perangkat komputer pribadi dengan berbagai cara tindakan berbahaya yang biasanya berasal dari sumber anonim yang mencuri, mengubah atau menghancurkan target yang ditentukan dengan cara membobol sistem yang rentan.[19] Ini dapat diberi label sebagai kampanye *cyber*, *cyberwarfare* atau *cyberterrorism* dalam konteks yang berbeda. *Cyberattacks* dapat berkisar dari menginstal *spyware* di PC untuk mencoba menghancurkan infrastruktur seluruh negara. *Cyberattacks* telah menjadi semakin canggih dan berbahaya seperti *worm Stuxnet* yang baru-baru ini didemonstrasikan.[20] Analisis perilaku pengguna dan Keamanan Informasi dan *Event* Manajemen (*Security Information and Eevent Management* / SIEM) digunakan untuk mencegah serangan ini. Pakar hukum berusaha membatasi penggunaan istilah tersebut pada insiden yang menyebabkan kerusakan fisik, membedakannya dari pelanggaran data yang lebih rutin dan aktivitas *hacking* yang lebih luas.[21]

Serangan sintaksis

Secara rinci, ada sejumlah teknik untuk memanfaatkan serangan *cyber* dan berbagai cara untuk mengelolanya kepada individu atau perusahaan dalam skala yang lebih luas. Serangan dibagi menjadi dua kategori: serangan sintaksis dan serangan semantik. Serangan sintaksis sangat mudah hanya menggunakan *software* berbahaya. *Software* berbahaya ini termasuk *virus*, *worm*, dan *trojan horse*.

- *Virus*
  Virus adalah program replikasi diri yang bisa menempel pada program

[17] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, ABC-CLIO, 2010, pp. 91

[18] *"We talked to the opportunist imitator behind Silk Road 3.0". 2014-11-07. Retrieved 2016-10-04.*

[19] Financial Weapons of War, 100 Minnesota Law Review 1377 (2016)

[20] S. Karnouskos: *Stuxnet Worm Impact on Industrial Cyber-Physical System Security.* In:*37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011), Melbourne, Australia*, 7-10 Nov 2011. Retrieved 20 Apr 2014.

[21] *SATTER, RAPHAEL (28 March 2017). "What makes a cyberattack? Experts lobby to restrict the term". Retrieved 7 July 2017.*

atau file lain agar bisa bereproduksi. *Virus* dapat bersembunyi dalam memori sistem komputer dan menempelkan dirinya ke *file* apa pun yang menurutnya sesuai untuk menjalankan kodenya. Hal ini juga dapat mengubah jejak digitalnya setiap kali bereplikasi sehingga sulit dilacak di kom-puter.

- *Worms*
  Worm tidak memerlukan file atau program lain untuk menyalin dirinya sendiri. Ini adalah program berjalan mandiri. *Worm* mereplikasi jaringan dengan menggunakan protokol. Inkarnasi *worm* terbaru memanfaatkan kerentanan yang diketahui dalam sistem untuk menembus, mengeksekusi kode mereka, dan meniru sistem lain seperti *worm Code Red II* yang menginfeksi lebih dari 259.000 sistem dalam waktu kurang dari 14 jam.[22] Pada skala yang jauh lebih besar, *worm* dapat dirancang untuk spionase industri, untuk memantau dan mengumpulkan data dari *server* lalu mengirimkannya kembali ke penciptanya.

- *Trojan Horse*
  Trojan horse dirancang untuk melakukan tugas yang seakan-akan sah namun juga melakukan aktivitas yang tidak diketahui dan tidak diinginkan. Ini bisa menjadi dasar dari banyaknya penyebaran *virus* dan *worm* yang menginstal ke komputer dan juga penyebaran *malicious software* seperti misalnya *keyboard logger* dan *backdoor software*. Dalam pengertian komersial, *Trojan horse* dapat tertanam dalam versi *trial* dari perangkat lunak dan dapat mengumpulkan informasi tambahan tentang target tanpa sepengetahuan orang yg jadi sasarannya.

Ketiga hal tersebut di atas cenderung menyerang individu dan/atau perusahaan melalui *email*, *web browser*, *chat clients*, *remote software* dan *updates*.

Serangan semantik
Serangan semantik adalah modifikasi dan penyebaran informasi yang benar dan salah. Informasi yang dimodifikasi bisa saja dilakukan tanpa menggunakan komputer meski peluang baru bisa ditemukan dengan menggunakan komputer. Untuk mengatur seseorang ke arah yang salah atau untuk menutupi jejak Anda, penyebaran informasi yang salah dapat digunakan.

KASUS TERDOKUMENTASI
- Salah satu kejahatan komputer perbankan berprofil tinggi terjadi selama tiga tahun dimulai pada tahun 1970. Kepala *teller* di cabang Park Avenue New York Union Dime Savings Bank menggelapkan lebih dari $ 1,5 juta dari ratusan akun.[23]
- Sebuah kelompok *hacking* bernama MOD (*Masters of Deception*), diduga mencuri *password* dan data teknis dari Pacific Bell, Nynex dan perusahaan telepon lainnya serta beberapa agensi kredit besar dan dua universitas besar. Kerusakan yang terjadi sangat luas, satu perusahaan, Southwestern Bell mengalami kerugian sebesar $ 370.000.[23]
- Pada tahun 1983, seorang siswa UCLA berusia sembilan belas tahun menggunakan PC-nya untuk masuk ke

[22] Janczewski, Lech, and Andrew Colarik. Cyber Warfare and Cyber Terrorism. Hershey, New York: Information Science Reference, 2008. Web.

[23] *Weitzer, Ronald (2003). Current Controversies in Criminology. Upper Saddle River, New Jersey: Pearson Education Press. p. 150.*

sistem komunikasi internasional Departemen Pertahanan.[23]

- Antara 1995 dan 1998, satelit Newscorp membayar untuk melihat layanan SKY-TV terenkripsi telah diretas beberapa kali selama perlombaan teknologi senjata yang sedang berlangsung antara kelompok *hacker* Eropa dan Newscorp. Motivasi awal para *hacker* adalah menonton filem *Star Trek re-runs* di Jerman, yang merupakan sesuatu pelanggaran hak cipta oleh Newscorp.[24]
- Pada tanggal 26 Maret 1999, *virus worm* Melissa menginfeksi dokumen di komputer korban, lalu secara otomatis mengirimkan dokumen tersebut dan salinan virus tersebut menyebar melalui *e-mail* ke orang lain.
- Pada bulan Februari 2000, seorang individu yang menggunakan nama alias MafiaBoy memulai serangkaian serangan *denial-of-service* terhadap situs *web* berprofil tinggi, termasuk Yahoo!, Amazon.com, Dell, Inc., E * TRADE, eBay dan CNN. Sekitar lima puluh komputer di Stanford University dan juga komputer di University of California di Santa Barbara, ada di antara komputer *zombie* yang mengirimkan ping pada serangan DDoS. Pada tanggal 3 Agustus 2000, jaksa federal Kanada menuntut MafiaBoy dengan 54 jumlah akses ilegal ke komputer, ditambah total sepuluh tuduhan kenakalan serangannya terhadap data.
- Jaringan Bisnis Rusia (RBN) terdaftar sebagai situs internet pada tahun 2006. Awalnya, sebagian besar aktivitasnya sah. Namun rupanya para pendiri perusahaan segera menemukan bahwa lebih menguntungkan untuk menjalankan kegiatan tidak sah dan mulai mempekerjakan jasanya kepada penjahat. RBN telah dijelaskan oleh *VeriSign* sebagai "*baddest of the bad*".[25] Menawarkan layanan *web hosting* dan akses *internet* untuk semua jenis aktivitas kriminal, dengan aktivitas individual menghasilkan hingga $150 juta dalam satu tahun. Dalam beberapa kasus memonopoli pencurian identitas pribadi untuk dijual kembali. Ini adalah pendiri MPack dan operator *botnet Storm* yang sekarang sudah tidak berfungsi lagi.
- Pada tanggal 2 Maret 2010, penyidik Spanyol menangkap 3 pelaku kejahatan komputer yang menyebabkan terinfeksinya lebih dari 13 juta komputer di seluruh dunia. Menurut penyidik tersebut, "*Botnet*" komputer yang terinfeksi termasuk PC di dalam lebih dari setengah aset 1000 perusahaan dan lebih dari 40 bank besar.
- Pada bulan Agustus 2010, penyelidikan internasional Operasi Delego, yang beroperasi di bawah naungan Departemen Keamanan Dalam Negeri, menutup jaringan pedofil internasional *Dreamboard*. Situs ini memiliki sekitar 600 anggota, dan mungkin telah mendistribusikan hingga 123 *terabyte* pornografi anak (kira-kira setara dengan 16.000 DVD). Sampai sekarang ini adalah penuntutan terbesar AS atas sebuah jaringan pornografi anak internasional. 52 penangkapan dilakukan di seluruh dunia.[26]
- Pada bulan Januari 2012 Zappos.com mengalami penyusupan keamanan setelah 24 juta nomor kartu kredit pe-

[24] *David Mann And Mike Sutton (2011-11-06). ">>Netcrime". Bjc.oxfordjournals.org. Retrieved 2011-11-10.*

[25] *"A walk on the dark side". The Economist. 2007-09-30.*

[26] *"DHS: Secretary Napolitano and Attorney General Holder Announce Largest U.S. Prosecution of International Criminal Network Organized to Sexually Exploit Children". Dhs.gov. Retrieved 2011-11-10.*

langgan, informasi pribadi, alamat penagihan dan pengiriman telah dicuri.[27]

- Pada bulan Juni 2012 *LinkedIn* dan *eHarmony* diserang, mengorbankan 65 juta *hash* kata sandi. 30.000 kata sandi telah berhasil dicuri dan 1,5 juta *password EHarmony* disebarkan secara *online*.[28]
- Desember 2012 situs Wells Fargo mengalami serangan DoS. Berpotensi mengorbankan 70 juta pelanggan dan 8,5 juta pemirsa aktif. Bank lain yang juga diperkirakan menjadi korban adalah Bank of America, JP Morgan US Bank dan PNC Financial Services.[29]
- 23 April 2013 akun *Twitter Associated Press* di-*hack. Hacker* membubuhkan *tweet hoax* tentang serangan fiktif di Gedung Putih (*The White House*) yang mereka klaim membuat Presiden Obama cedera.[30] *Tweet hoax* ini menyebabkan penurunan singkat 130 poin dari saham Dow Jones Industrial, menghapus $136 miliar dari indeks S&P 500,[31] dan penghentian sementara akun *Twitter Associated Press*. Dow Jones kemudian memulihkan kembali akun tersebut..
- Pada bulan Mei 2017, 74 negara mencatat sebuah *cybercrime ransomware*, yang disebut "*WannaCry*"[32]

[27] *DAVID K. LI (January 17, 2012). "Zappos cyber attack". New York Post.*
[28] *Salvador Rodriguez (June 6, 2012). "Like LinkedIn, eHarmony is hacked; 1.5 million passwords stolen". Los Angeles Times.*
[29] *Rick Rothacker (Oct 12, 2012). "Cyber attacks against Wells Fargo "significant," handled well: CFO". Reuters.*
[30] *"AP Twitter Hack Falsely Claims Explosions at White House". Samantha Murphy. April 23, 2013. Retrieved April 23, 2013.*
[31] *"Fake Tweet Erasing $136 Billion Shows Markets Need Humans". Bloomberg. April 23, 2013. Retrieved April 23, 2013.*
[32] *hermesauto (13 May 2017). "Unprecedented cyber attacks wreak global havoc".*

MEMERANGI KEJAHATAN KOMPUTER

Difusi *cybercrime*

Difusi luas aktivitas *cybercriminal* adalah masalah dalam deteksi dan penuntasan kejahatan komputer. Menurut Jean-Loup Richet (*Research Fellow* di ESSEC ISIS), keahlian teknis dan aksesibilitas tidak lagi bertindak sebagai penghalang masuk ke *cybercrime*.[33] Memang, *hacking* jauh lebih rumit daripada beberapa tahun yang lalu, karena komunitas *hacker* telah menyebarkan pengetahuan mereka melalui Internet. *Blog* dan komunitas *hacker* sangat berkontribusi dalam berbagi informasi: seorang *hacker* pemula bisa mendapatkan keuntungan dari pengetahuan dan saran dari *hacker* yang lebih senior.

Selanjutnya, *hacking* lebih murah dari sebelumnya: sebelum era *cloud computing*, untuk *spam* atau *scam* dibutuhkan *server* yang berdedikasi, ketrampilan dalam manajemen *server*, konfigurasi jaringan dan pemeliharaan, pengetahuan tentang standar penyedia layanan Internet dan lain-lain.

Sebagai perbandingan, *mail software-as-a-service* adalah layanan pengiriman *email* terukur, murah, massal dan transaksional untuk tujuan pemasaran dan dapat dengan mudah disiapkan untuk *spam*.[34] Jean-Loup Richet menjelaskan bahwa *cloud computing* dapat membantu *cybercriminal* sebagai cara untuk memanfaatkan serangannya - *brute-force password*, meningkatkan jangkauan *botnet*

[33] *Richet, Jean-Loup (2013). "From Young Hackers to Crackers". International Journal of Technology and Human Interaction. **9** (1).*
[34] *Richet, Jean-Loup (2011). "Adoption of deviant behavior and cybercrime 'Know how' diffusion". York Deviancy Conference.*

atau memfasilitasi kampanye *spamming*.[35]

Investigasi

Komputer bisa menjadi sumber bukti (forensik digital). Bahkan di mana komputer tidak digunakan secara langsung untuk tujuan kriminal, catatan itu mungkin berisi catatan nilai bagi penyidik kriminal dalam bentuk *logfile*. Di kebanyakan negara penyedia layanan internet (*Internet Service Providers*) secara hukum diharuskan untuk menyimpan *logfiles* mereka untuk jumlah waktu yang telah ditentukan. Sebagai contoh; Petunjuk Penyimpanan Data Eropa yang luas (berlaku untuk semua negara anggota Uni Eropa) menyatakan bahwa semua lalu lintas *E-mail* harus dipertahankan minimal selama 12 bulan.

- Metodologi investigasi *cybercrime*
  Ada banyak cara untuk kejahatan dunia maya bisa terjadi dan penyelidikan cenderung dimulai dengan jejak alamat IP (*IP Address*), namun itu belum tentu merupakan basis faktual dimana penyidik dapat menyelesaikan sebuah kasus. Berbagai jenis kejahatan teknologi tinggi mungkin juga mencakup unsur-unsur kejahatan teknologi rendah dan sebaliknya, membuat penyidik dunia maya menjadi bagian tak terpisahkan dari penegakan hukum modern. Metodologi kerja penyidik *cybercrime* bersifat dinamis dan terus membaik, baik di unit polisi khusus, maupun dalam kerangka kerjasama internasional.[36]

Legislasi

Karena undang-undang yang mudah dieksploitasi, penjahat dunia maya menggunakan negara-negara berkembang untuk menghindari deteksi dan penuntutan dari penegak hukum. Di negara berkembang, seperti Filipina, hukum melawan *cybercrime* sangat lemah atau terkadang tidak ada. Undang-undang yang lemah ini memungkinkan penjahat dunia maya menyerang dari perbatasan internasional dan tetap tidak terdeteksi. Bahkan ketika diidentifikasi, penjahat ini menghindari hukuman atau ekstradisi ke negara lain, seperti Amerika Serikat, yang telah mengembangkan undang-undang yang memungkinkan penuntutan.

Meskipun hal ini terbukti sulit dalam beberapa kasus, agensi seperti FBI, telah menggunakan tipu muslihat dan dalih untuk menangkap penjahat. Sebagai contoh; dua *hacker* Rusia telah menghindari FBI untuk beberapa lama. FBI mendirikan sebuah perusahaan komputasi palsu yang berbasis di Seattle, Washington. Mereka melanjutkan untuk memancing dua pria Rusia ke Amerika Serikat dengan menawarkan mereka bekerja dengan perusahaan ini. Setelah selesai wawancara, tersangka ditangkap di luar gedung. Trik pintar seperti ini terkadang merupakan bagian penting dari penangkapan penjahat dunia maya saat undang-undang yang lemah membuat hal itu menjadi tidak mungkin lain.[37]

Presiden Barack Obama mengeluarkan perintah eksekutif pada bulan April 2015 untuk memerangi kejahatan dunia maya. Perintah eksekutif ini memungkinkan Amerika Serikat untuk membekukan aset kejahatan dunia maya dan memblokir

[35] *Richet, Jean-Loup (2012). "How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry Into Cybercrime". 17th AIM Symposium.*

[36] http://www.unafei.or.jp/english/pdf/RS_No79/No79_15RC_Group2.pdf

[37] *Kshetri, Nir. "Diffusion and Effects of Cyber Crime in Developing Countries".*

aktivitas ekonomi mereka di Amerika Serikat. Ini adalah beberapa undang-undang padat pertama yang memerangi *cybercrime* dengan cara ini.[38]

Uni Eropa mengadopsi arahan 2013/40/EU. Semua pelanggaran terhadap direktif tersebut dan institusi prosedural lainnya juga ada dalam Konvensi Dewan Eropa tentang *Cybercrime*.[39]

Hukuman

Sanksi untuk kejahatan terkait komputer di Negara Bagian New York dapat berkisar dari denda dan masa hukuman penjara yang singkat untuk pelanggaran ringan Kelas A seperti penggunaan komputer yang tidak sah sampai gangguan komputer pada tingkat pertama yang merupakan tindak pidana Kelas C dan dapat dilakukan. 3 sampai 15 tahun penjara. Namun, beberapa *hacker* telah dipekerjakan sebagai pakar keamanan informasi oleh perusahaan swasta karena pengetahuan mereka tentang kejahatan komputer, sebuah fenomena yang secara teoritis dapat menciptakan insentif yang menyimpang.

Kemungkinan penghindaran ini adalah agar pengadilan melarang para *hacker* yang dipidana menggunakan komputer dan internet dalam bentuk apapun, bahkan setelah mereka dibebaskan dari penjara, meskipun saat komputer dan internet menjadi sangat lebih penting bagi kehidupan sehari-hari, hukuman jenis ini dapat artikan sebagai hukuman lebih keras dan kejam. Namun, pendekatan lain telah dikembangkan untuk me-*manage* para pelaku kejahatan *cyber* tanpa larangan total dalam menggunakan komputer atau internet.[40] Pendekatan ini melibatkan pembatasan individu terhadap perangkat tertentu yang dapat dilakukan dengan cara pemantauan komputer atau penelusuran komputer oleh petugas percobaan atau pembebasan bersyarat.[41]

KESIMPULAN

Seiring kemajuan teknologi dan lebih banyak orang mengandalkan internet untuk menyimpan informasi sensitif seperti informasi kartu kredit atau perbankan, penjahat akan berusaha mencuri informasi itu. Kejahatan *cyber* menjadi lebih merupakan ancaman bagi orang di seluruh dunia. Meningkatkan kesadaran tentang bagaimana informasi dilindungi dan mengetahui taktik yang digunakan penjahat *cyber* untuk mencuri informasi itu penting di dunia sekarang ini. Menurut Pusat Pengaduan Kejahatan Internet FBI pada tahun 2014 ada 269.422 keluhan yang diajukan. Dengan semua klaim gabungan terjadi kerugian total yang dilaporkan sebesar $800.492.073.[42] Tapi kejahatan *cyber* sepertinya tidak diketahui oleh kebanyakan orang.

Ada 1,5 juta serangan *cyber* setiap tahunnya, itu berarti ada lebih dari 4.000 serangan sehari, 170 serangan setiap jam, atau hampir tiga serangan setiap menit, dengan penelitian menunjukkan bahwa

[38] *Northam, Jackie. "U.S. Creates First Sanctions Program Against Cybercriminals".*

[39] *Adrian Cristian MOISE (2015). "Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level" (PDF). Journal of Law and Administrative Sciences. Archived from the original (PDF) on December 8, 2015.*

[40] *"Managing the Risks Posed by Offender Computer Use - Perspectives" (PDF). December 2011.*

[41] *Bowker, Art (2012). The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st Century. Springfield: Thomas. ISBN 9780398087289.*

[42] *"2014 Internet Crime Report" (PDF). Internet Crime Complaint Center (IC3). 2015. Retrieved 2017-10-31.*

hanya 16% korban telah meminta orang-orang yang melakukan serangan untuk menghentikan serangannya.[43] Siapa saja yang menggunakan internet karena alasan apapun bisa menjadi korban, karena itu-lah penting untuk mengetahui bagaimana seseorang dilindungi saat *online*.

REFERENSI

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S. & Zarsky, T. (2006) (eds) *Cybercrime: Digital Cops in a Networked Environment*, New York University Press, New York.

Bowker, Art (2012) "The Cybercrime Handbook for Community Corrections: Managing Risk in the 21st Century" Charles C. Thomas Publishers, Ltd. Springfield.

Brenner, S. (2007) *Law in an Era of Smart Technology,* Oxford: Oxford University Press

Broadhurst, R., and Chang, Lennon Y.C. (2013) "Cybercrime in Asia: trends and challenges", in B. Hebenton, SY Shou, & J. Liu (eds), Asian Handbook of Criminology (pp. 49–64). New York: Springer (ISBN 978-1-4614-5217-1)

Chang, L.Y. C. (2012) *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. Cheltenham: Edward Elgar. (ISBN 978-0-85793-667-7)

Chang, Lennon Y.C., & Grabosky, P. (2014) "Cybercrime and establishing a secure cyber world", in M. Gill (ed) Handbook of Security (pp. 321–339). NY: Palgrave.

Csonka P. (2000) Internet Crime; the Draft council of Europe convention on cyber-crime: A response to the challenge of crime in the age of the internet? *Computer Law & Security Report* Vol.16 no.5.

Easttom C. (2010) *Computer Crime Investigation and the Law*

Fafinski, S. (2009) *Computer Misuse: Response, regulation and the law* Cullompton: Willan

Glenny, Misha, *DarkMarket : cyberthieves, cybercops, and you*, New York, NY : Alfred A. Knopf, 2011. ISBN 978-0-307-59293-4

Grabosky, P. (2006) *Electronic Crime*, New Jersey: Prentice Hall

Halder, D., & Jaishankar, K. (2016). Cyber Crimes against Women in India. New Delhi: SAGE Publishing. ISBN 978-9385985775.

Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

Jaishankar, K. (Ed.) (2011). Cyber Criminology: Exploring Internet Crimes and Criminal behavior. Boca Raton, FL, USA: CRC Press, Taylor and Francis Group.

McQuade, S. (2006) *Understanding and Managing Cybercrime*, Boston: Allyn & Bacon.

McQuade, S. (ed) (2009) *The Encyclopedia of Cybercrime*, Westport, CT: Greenwood Press.

[43] *Feinberg, T (2008). "Whether it happens at school or off-campus, cyberbullying disrupts and affects". Cyberbullying: 10.*

Parker D (1983) *Fighting Computer Crime*, U.S.: Charles Scribner's Sons.

Pattavina, A. (ed) *Information Technology and the Criminal Justice System*, Thousand Oaks, CA: Sage.

Paul Taylor. Hackers: Crime in the Digital Sublime (November 3, 1999 ed.). Routledge; 1 edition. p. 200. ISBN 0-415-18072-4.

Robertson, J. (2010, March 2). Authorities bust 3 in infection of 13m computers. Retrieved March 26, 2010, from Boston News: Boston.com

Walden, I. (2007) *Computer Crimes and Digital Investigations*, Oxford: Oxford University Press.

Rolón, Darío N. Control, vigilancia y respuesta penal en el ciberespacio, Latin American's New Security Thinking, Clacso, 2014, pp. 167/182

Richet, J.L. (2013) From Young Hackers to Crackers, *International Journal of Technology and Human Interaction (IJTHI)*, 9(3), 53-62.

Wall, D.S. (2007) *Cybercrimes: The transformation of crime in the information age*, Cambridge: Polity.

Williams, M. (2006) *Virtually Criminal: Crime, Deviance and Regulation Online*, Routledge, London.

Yar, M. (2006) *Cybercrime and Society*, London: Sage